IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

MICHAEL CASTELLANO, ANITA OHREN, CURTIS BARNARD, DORIS CURRY, and AMY MAYLORD, on behalf of themselves and all others similarly situated,	)	Case No.
Plaintiffs,	)	JURY TRIAL DEMANDED
vs.	)	
SCHNUCK MARKETS, INC., a Missouri corporation,	)	
Defendant.	)	

CLASS ACTION COMPLAINT

NOW COME the Plaintiffs, on behalf of themselves and all others similarly situated, and for their class action complaint state as follows:

NATURE OF THE ACTION

1. Plaintiffs bring this class action as a result of a breach of the security system of Defendant Schnuck Markets, Inc. ("Schnucks") governing electronic transactions, resulting in compromised security of Plaintiffs' and Class Members' personal financial information. Upon information and belief, such personal information includes credit and debit card information, personal identification numbers ("PINs") and Plaintiffs' and putative Class Members' names ("Personal Information").

2. Schnucks has admitted publicly that between December 1, 2012, and March 29, 2013, approximately 2.4 million credit and debit cards used at 79 of the 100 stores Schnucks operates in Missouri, Illinois, Indiana, Iowa, and Wisconsin, were compromised, with the result that Personal Information of Plaintiffs and Class Members was used in fraudulent transactions around the world.

3. As early as mid-March 2012, Schnucks learned that its computer systems had been compromised, allowing one or more individuals to steal Plaintiffs' and putative Class Members' Personal Information when several individuals reported fraudulent charges on their credit or debit cards when shopping at Schnucks, yet Schnucks made no attempt to inform consumers of the breach until substantially later.

4. The security breach and theft of Personal Information was caused by Schnucks's violations of its obligations to abide by the best practices and industry standards concerning the security of its payment processing systems and the computers associated therewith as set forth, for example, in Payment Card Industry Security Standards Council Data Security Standards ("PCI DSS") and the decisions of the Federal Trade Commission ("FTC") concerning protection of consumer financial information.

5. After learning of the security breach, Schnucks failed to notify Plaintiffs and the putative Classes in a timely manner and failed to take other reasonable steps to inform them of the nature and extent of the breach. As a result, Schnucks prevented Plaintiffs and the putative Class Members from protecting themselves from the breach and caused Plaaintiffs and Class Members to suffer financial loss.

6. Plaintiffs, on behalf of themselves and all others similarly situated, assert the following claims: violations of the Stored Communications Act ("SCA"), 18 U.S.C. § 2702; negligence; breach of implied contract; violations of the Missouri Merchandising Practices Act ("MMPA"), Mo. Rev. Stat. § 407.020, and the substantially similar statutes of the other states in which Schnucks conducts business; and violations of the Illinois Personal Information Protection Act ("IPIPA"), 815 ILCS 530/1, and the substantially similar statutes of the other states in which Schnucks conducts business.

JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331, which confers upon the Court original jurisdiction over all civil actions arising under the laws of the United States, and pursuant to 18 U.S.C. § 2707. This Court has supplemental jurisdiction over Plaintiffs' and Class Members' state law claims under 28 U.S.C. § 1367.

8. In addition, this Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all Members of the putative Classes are in excess of $5,000,000.00, exclusive of interest and costs, and many of the Members of the putative Classes are citizens of different states than Defendant. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d).

9. Venue is properly set in this District pursuant to 28 U.S.C. § 1391(b) since Schnucks resides in this judicial district, transacts business, and is found within this judicial district. Likewise, a substantial part of the events giving rise to the claim occurred within this judicial district.

PARTIES

10. Plaintiff Michael Castellano is domiciled in St. Louis, Missouri, and is a citizen of Missouri. Between December 2012 and March 2013, Castellano shopped at Schnucks in St. Louis and swiped his debit card through a Schnucks pin pad terminal. Castellano's Personal Information was compromised and unauthorized charges in the amount of approximately $197 appeared on his debit card account. Castellano was forced to cancel his debit card and incurred a non-refundable $20 fee to procure a replacement debit card.

11. Plaintiff Anita Ohren is domiciled in Moline, Illinois, and is a citizen of Illinois. Between December 2012 and March 2013, Ohren shopped at Schnucks in Davenport, Iowa, and

swiped her credit/debit card through a Schnucks pin pad terminal. Ohren's Personal Information was compromised and unauthorized charges in the amount of approximately $300 appeared on her credit/debit card account. Ohren was forced to cancel her credit/debit card and was unable to recover the $300 in unauthorized charges on her card that resulted from the breach of Schnucks computer security.

12. Plaintiff Curtis Barnard is domiciled in Newburgh, Indiana, and is a citizen of Indiana. Between December 2012 and March 2013, Barnard shopped at Schnucks in Evansville, Indiana, and swiped his credit/debit card through a Schnucks pin pad terminal. Barnard's Personal Information was compromised and unauthorized charges in the amount of approximately $600 appeared on his credit/debit card account. Barnard was forced to take time off from work in order to cancel his credit/debit card and was without a credit/debit card for approximately 4 days.

13. Plaintiff Doris Curry is domiciled in Davenport, Iowa, and is a citizen of Iowa. Between December 2012 and March 2013, Curry shopped at Schnucks in Davenport, Iowa, and swiped her credit/debit card through a Schnucks pin pad terminal. Curry's Personal Information was compromised and unauthorized charges appeared on her credit/debit card account.

14. Plaintiff Amy Maylord is domiciled in Jamesville, Wisconsin, and is a citizen of Wisconsin. Between December 2012 and March 2013, Maylord shopped at Schnucks in Madison, Wisconsin, and swiped her credit/debit card through a Schnucks pin pad terminal. Maylord's Personal Information was compromised and an unauthorized charge in the amount of approximately $40 appeared on her credit/debit card account. Maylord was forced to cancel her credit/debit card.

15. Schnucks is a corporation organized under Missouri law with its headquarters and principal place of business in St. Louis, Missouri, and therefore is a citizen of Missouri. Schnucks owns and operates 100 supermarkets throughout Illinois, Missouri, Indiana, Iowa, and Wisconsin.

FACTUAL BACKGROUND

16. Schnucks accepts customer payments for purchase through credit and debit cards issued by members of the payment card industry ("PCI") such as Visa or MasterCard.

17. In 2006, the PCI members established a Security Standards Counsel ("PCI SSC") as a forum to develop PCI Data Security Standards ("PCI DSS") for increased security of payment processing systems.

18. The PCI DSS provides, "If you are a merchant that accepts payment cards, you are required to be compliant with the PCI Data Security Standard." Schnucks is a merchant that accepts payment cards.

19. The PCI DSS requires a merchant to:

a. **Assess**—identify cardholder data, take inventory of IT assets and business processes for payment card processing, and analyze them for vulnerabilities that could expose cardholder data.

b. **Remediate**—fix vulnerabilities and do not store cardholder data unless needed.

c. **Report**—compile and submit required remediation validation records (if applicable) and submit compliance reports to the acquiring bank and card brands with which a merchant does business.

20. Additionally, since 1995, the FTC has been studying the manner in which online entities collect and use personal information and safeguards to assure that online data collection practice is fair and provides adequate information privacy protection. The result of this study is the FTC Fair Information Practice Principles. The core principles are:

a. **Notice/Awareness**--Consumers should be given notice of an entity's information practices before any personal information is collected from them. This requires that companies explicitly notify of some or all of the following:

- Identification of the entity collecting the data;
- Identification of the uses to which the data will be put;
- Identification of any potential recipients of the data;
- The nature of the data collected and the means by which it is collected;
- Whether the provision of the requested data is voluntary or required; and
- The steps taken by the data collector to ensure the confidentiality, integrity and quality of the data.

b. **Choice/Consent**--Choice and consent in an online information-gathering sense means giving consumers options to control how their data is used with respect to secondary uses of information beyond the immediate needs of the information collector to complete the consumer's transaction.

c. **Access/Participation**--Access as defined in the Fair Information Practice Principles includes not only a consumer's ability to view the data collected, but also to verify and contest its accuracy. This access must be inexpensive and timely in order to be useful to the consumer.

d. **Integrity/Security**--Information collectors should ensure that the data they collect is accurate and secure. They should improve the integrity of data by cross-referencing it with only reputable databases and by providing access for the consumer to verify it. Information collectors should keep their data secure by protecting against both internal and external security threats. They should limit access within their company to only necessary employees to protect against internal threats, and they should use encryption and other computer-based security systems to stop outside threats.

e. **Enforcement/Redress--**In order to ensure that companies follow the Fair Information Practice Principles, there must be enforcement measures. The FTC identifies three types of enforcement measures: self-regulation by the information collectors or an appointed regulatory body; private remedies that give civil causes of action for individuals whose information has been misused to sue violators; and government enforcement, which can include civil and criminal penalties levied by the government.

21. On information and belief, Schnucks failed adequately to analyze its computer systems for vulnerabilities that could expose cardholder data. Schnucks further failed to fix the vulnerabilities in its computer systems which allowed Plaintiffs' and Class Members' Personal Information to become compromised.

22. Additionally, on information and belief, Schnucks unlawfully collected consumer financial data for marketing purposes beyond the needs of specific transactions, in order to accrue financial benefit at the risk and likelihood of compromising consumers' Personal Information.

23. As a result, Schnucks allowed all the information contained on the magnetic strips on the backs of the Plaintiffs' and Class Members' credit cards and debit cards to become

compromised in at least 79 of its 100 stores for a minimum period of between December 2012 until March 2013.

24. On March 15, 2013, Schnucks learned that at least 12 credit or debit cards were subject to fraud complaints after consumers had shopped at Schnucks. On March 19, 2013, Schnucks was aware that additional cards were also subject to fraud after consumers made purchases at Schnucks stores.

25. On March 28, 2013, Schnucks was able to determine that through the use of malware one or more individuals were able to obtain Plaintiffs' and Class Members' Personal Information.

26. Schnucks has estimated that approximately 2.4 million customer cards have been compromised as a result of this security breach.

27. Despite having such knowledge as early as March 15, 2013, that customers were experiencing fraud with regard to their credit cards and/or debit cards used to purchase goods at Schnucks, Defendant did not inform any customers of the fraud until a significantly later date. Moreover, at that time Schnucks only told customers its computer systems had been compromised and the issue was "found and contained."

28. To date, Schnucks has not provided individual notification to Plaintiffs and Class Members of the security breach.

29. Also, to date, Schnucks has not reimbursed Plaintiffs and Class Members for financial losses caused by the security breach.

30. Plaintiffs and Class Members are subject to continuing damage from having their Personal Information comprised as a result of Schnucks' inadequate systems. Such damages include, among other things, out-of-pocket expenses incurred to mitigate the increased risk of

identity theft and or fraud, the value of their time and resources spent mitigating the identity theft and/or fraud, the cost of and time spent replacing credit cards and debit cards and reconfiguring automatic payment programs with other merchants related to the compromised cards, and irrecoverable financial losses due to unauthorized charges on the credit/debit cards of Schnucks customers by identity thieves who wrongfully gained access to the Personal Information of Plaintiffs and the Classes.

CLASS ACTION ALLEGATIONS

31. Plaintiffs bring this action on their own behalf and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following two (2) multi-state classes:

> All persons who shopped at Defendant's locations, who were not provided notice of the data breach of Defendant's security that compromised consumers' credit card and debit card information and who suffered damages in the loss of time and use of their credit and debit cards until such time as replacement cards could be obtained.
>
> All persons who shopped at Defendant's locations, who were not provided notice of the data breach of Defendant's security that compromised consumers' credit card and debit card information and suffered damages in the amount of fraudulent charges made to their credit and/or debit cards not reimbursed or reversed by their financial institution or suffered damages in the amount of overdraft charges made to their credit and/or debit cards not reimbursed or reversed by their financial institution.

Excluded from the Classes are Schnucks and its affiliates, parents, subsidiaries, employees, officers, agents, and directors.

32. The Members of the Classes are so numerous that joinder of all Members is impracticable. Schnucks has publicly admitted that up to 2.4 million credit and/or debit cards may have been compromised, and the Members of the Classes are geographically dispersed. Disposition of the claims of the proposed Classes in a class action will provide substantial benefits to both the parties and the Court.

33. The rights of each member of the proposed Classes were violated in a similar fashion based upon Schnucks' uniform wrongful actions and/or inaction.

34. The following questions of law and fact are common to each proposed Class Member and predominate over questions that may affect individual Class Members:

a. Whether Schnucks failed to use reasonable care and commercially reasonable methods to secure and safeguard its customers' private financial information;

b. Whether Schnucks properly implemented its purported security measures to protect consumers' private financial information from unauthorized capture, dissemination and misuse;

c. Whether Schnucks took reasonable measures to determine the extent of the security breach after it first learned of the same;

d. Whether Schnucks' delay in informing consumers of the security breach was unreasonable;

e. Whether Schnucks' method of informing consumers of the security breach and its description of the breach and potential exposure to damages as a result of the same was unreasonable;

f. Whether Schnucks' conduct violated the Stored Communications Act, 18 U.S.C. § 2702;

g. Whether Schnucks breached an implied contract with Class Members;

h. Whether Schnucks' conduct violated the Missouri Merchandising Practices Act, Mo. Rev. Stat. § 407.020, and the substantively similar statutes of the other states where Schnucks conducts business;

i. Whether Schnucks' conduct violated the Illinois Personal Information Protection Act, 815 ILCS 530/1, and the substantially similar statutes of the other states in which Schnucks conducts business; and

j. Whether Plaintiffs and others Members of the Classes are entitled to compensation, monetary damages, and injunctive relief, and, if so, the nature and amount of such relief.

35. Plaintiffs' claims are typical of the claim of absent Class Members. If brought individually, the claim of each Class Member would necessarily require proof of the same material and substantive facts, and seek the same remedies.

36. The Plaintiffs are willing and prepared to serve the Court and the proposed Classes in a representative capacity. The Plaintiffs will fairly and adequately protect the interest of the Classes and have no interests adverse to, or which directly and irrevocably conflicts with, the interests of other Members of the Classes. Further, Plaintiffs have retained counsel experienced in prosecuting complex class action litigation.

37. Schnucks has acted or refused to act on grounds generally applicable to the proposed Classes, thereby making appropriate equitable relief with respect to the Classes.

38. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual claims by the Class Members are impractical, as the costs of prosecution may exceed what any Class Member has at stake.

39. Members of the Classes are readily ascertainable through Schnucks' records of the purchases made at its stores.

40. Prosecuting separate actions by individual Class Members would create a risk of inconsistent or varying adjudications that would establish incomparable standards of conduct for

Schnucks. Moreover, adjudications with respect to individual Class Members would, as a practical matter, be dispositive of the interests of other Class Members.

CAUSES OF ACTION

COUNT I – VIOLATION OF THE FEDERAL STORED COMMUNICATIONS ACT, 18 U.S.C. § 2702

41. Plaintiffs repeat, reallege, and incorporate paragraphs 1-40 in this Complaint as if fully set forth herein.

42. The Stored Communications Act ("SCA") contains provisions that provide consumers with redress if a company mishandles their electronically stored information. The SCA was designed, in relevant part, "to protect individuals' privacy interests in personal and proprietary information." S. Rep. No. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555 at 3557.

43. Section 2702(a)(1) of the SCA provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1).

44. The SCA defines "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." *Id*. at § 2510(15).

45. Through its payment processing equipment, Schnucks provides an "electronic communication service to the public" within the meaning of the SCA because it provides consumers at large with credit and debit card payment processing capability that enables them to send or receive wire or electronic communications concerning their private financial information to transaction managers, card companies, or banks.

46. By failing to take commercially reasonable steps to safeguard sensitive private financial information, even after Schnucks was aware that customers' Personal Information had been compromised, Schnucks has knowingly divulged customers' private financial information that was communicated to financial institutions solely for customers' payment verification purposes, while in electronic storage in Schnucks' payment system.

47. Section 2702(a)(2)(A) of the SCA provides that "a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service." 18 U.S.C. § 2702(a)(2)(A).

48. The SCA defines "remote computing service" as "the provision to the public of computer storage or processing services by means of an electronic communication system." 18 U.S.C. § 2711(2).

49. An "electronic communications systems" is defined by the SCA as "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." 18 U.S.C. § 2510(4).

50. Schnucks provides remote computing services to the public by virtue of its computer processing services for consumer credit and debit card payments, which are used by customers and carried out by means of an electronic communications system, namely the use of wire, electromagnetic, photooptical or photoelectric facilities for the transmission of wire or

electronic communications received from, and on behalf of, the customer concerning customer private financial information.

51. By failing to take commercially reasonable steps to safeguard sensitive private financial information, Schnucks has knowingly divulged customers' private financial information that was carried and maintained on Schnucks' remote computing service solely for the customer's payment verification purposes.

52. As a result of Schnucks' conduct described herein and its violations of Section 2702(a)(1) and (2)(A), Plaintiffs and putative Class Members have suffered injuries, including lost money and the costs associated with the need for vigilant credit monitoring to protect against additional identity theft. Plaintiffs, on their own behalf and on behalf of the putative Classes, seek an order awarding themselves and the Classes the maximum statutory damages available under 18 U.S.C. § 2707 in addition to the cost for 3 years of credit monitoring services.

COUNT II – NEGLIGENCE

53. Plaintiffs repeat, reallege, and incorporate paragraphs 1-40 in this Complaint as if fully set forth herein.

54. Upon coming into possession of Plaintiffs' and Class Members' Personal Information, i.e., private, non-public, sensitive financial information, Schnucks had (and continues to have) a duty to exercise reasonable care in safeguarding and protecting the information from being compromised and/or stolen.

55. Schnucks also had a duty to timely disclose to Plaintiffs and Class Members that a breach of security had occurred and their Personal Information pertaining to their credit cards and/or debit cards had been compromised, or was reasonably believed to be compromised.

56. Schnucks also had a duty to put into place internal policies and procedures designed to detect and prevent the theft or dissemination of Plaintiffs' and Class Members' Personal Information.

57. Schnucks, by and through its above negligent acts and/or omissions, breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding their Personal Information which was in Schnucks' possession, custody, and control.

58. Schnucks, by and through its above negligent acts and or omissions, further breached its duty to Plaintiffs and Class Members by failing to put into place internal policies and procedures designed to detect and prevent the unauthorized dissemination of Plaintiffs and Class Members' Personal Information.

59. Schnucks, by and through its above negligent acts and or omissions, breached its duty to timely disclose the fact that Plaintiffs' and Class Members' Personal Information had been or was reasonable believed to be have been compromised.

60. But for Schnucks' negligent and wrongful breach of its duties owed to Plaintiffs and Class Members, their Personal Information would not have been compromised.

61. Plaintiffs' and Class Members' Personal Information was compromised and/or stolen as a direct and proximate result of Schnucks' breach of its duties as set forth herein.

62. Plaintiffs and Class Members have suffered actual damages including, but not limited to, having their personal information compromised, incurring time and expenses in cancelling their debit and/credit cards, activating new cards and re-establishing automatic payment authorizations from their new cards, and other economic and non-economic damages, including irrecoverable losses due to unauthorized charges on their credit/debit cards.

COUNT III -- BREACH OF IMPLIED CONTRACT

63. Plaintiffs repeat, reallege, and incorporate paragraphs 1-40 in this Complaint as if fully set forth herein.

64. Plaintiffs and Class Members were required to provide Schnucks with their Personal Information in order to facilitate their credit card and/or debit card transactions.

65. Implicit in this requirement was a covenant requiring Schnucks to take reasonable efforts to safeguard this information and promptly notify Plaintiffs and Class Members in the event their information was compromised.

66. Similarly, it was implicit that Schnucks would not disclose Plaintiffs' and Class Members' Personal Information.

67. Notwithstanding its obligations, Schnucks knowingly failed to safeguard and protect Plaintiffs' and Class Members' Personal Information. To the contrary, Schnucks allowed this information to be disseminated to unauthorized third parties.

68. Schnucks' above wrongful actions and/or inaction breached its implied contracts with Plaintiffs and Class Members, which in turn directly and/or proximately caused Plaintiffs and Class Members to suffer substantial injuries.

COUNT IV – VIOLATION OF THE MISSOURI MERCHANDISING PRACTICES ACT AND SUBSTANTIALLY SIMILAR STATUTES OF THE OTHER STATES WHERE DEFENDANT DOES BUSINESS

69. Plaintiffs repeat, reallege, and incorporate paragraphs 1-40 in this Complaint as if fully set forth herein.

70. Schnucks violated the Missouri Merchandising Practices Act, Mo. Rev. Stat. § 407.020, and the substantially similar statutes of the other states in which it conducts business by failing to properly implement adequate, commercially reasonable security measures to protect

customers' private financial information, and by failing to immediately notify affected customers of the nature and extent of the security breach.

71. Schnucks' fraudulent and deceptive omissions and misrepresentations regarding the company's security measures to protect customers' private financial information and the extent of the breach of those security measures were intended to deceive and induce Plaintiffs and the putative Class Members' reliance on Schnucks' misrepresentations that their financial information was secure and protected when using debit and credit cards to shop at Schnucks' stores.

72. Schnucks' unlawful misrepresentations and omissions occurred in the course of conduct involving trade or commerce.

73. Schnucks' unlawful misrepresentations and omissions were material because Plaintiffs and the other putative Class Members, if they had known the truth, would not have risked compromising their private financial information by using their debit or credit cards at Schnucks stores. Plaintiffs and the other putative Class Members would consider the omitted and misrepresented material facts important in making their purchasing decisions.

74. Schnucks' unlawful misrepresentations and omissions damaged Plaintiffs and the other putative Class Members because Plaintiffs and Class Members would not have chosen to expose their private financial information to a security breach and subsequent exploitation by the defrauders.

75. Plaintiffs, individually and on behalf of the putative Classes, seek an order requiring Defendant to pay: monetary and punitive damages for the conduct described herein; three years of credit card fraud monitoring services for Plaintiffs and Members of the putative

Classes; and the reasonable attorney's fees and costs of suit of Plaintiffs and Class Members; together with all such other and further relief as may be just.

COUNT V -- VIOLATION OF THE ILLINOIS PERSONAL INFORMATION PROTECTION ACT AND SUBSTANTIALLY SIMILAR STATUTES OF THE OTHER STATES WHERE DEFENDANT DOES BUSINESS

76. Plaintiffs repeat, reallege, and incorporate paragraphs 1-40 in this Complaint as if fully set forth herein.

77. At all times relevant hereto, there was in full force and effect the Illinois Personal Information Protection Act (IPIPA), 815 ILCS 530/1, together with other relevant state statutes providing that any data collector that owns or licenses personal information concerning a state resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach.

78. The relevant statutes provide that disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

79. Schnucks is a data collector within the meaning of the IPIPA and other relevant statutes.

80. Schnucks came into possession of Plaintiffs' and Class Members' personal information, as that is defined by the IPIPA and other relevant statutes.

81. Schnucks had a duty to disclose in the most expedient time possible and without unreasonable delay the breach of the security of the system data.

82. Schnucks, through its actions and/or omissions, failed to disclose in the most expedient time possible and without unreasonable delay the breach of the security of the system data.

83. Schnucks' failure to timely disclose is a violation of the IPIPA and other relevant statutes.

84. Plaintiffs and Class Members request that an injunction be issued to require Schnucks to comply with the IPIPA and other relevant statutes.

85. To the extent that a violation of the IPIPA and other relevant statutes also constitutes a violation of pertinent state consumer protection laws, *see, e.g.*, Section 20 of the IPIPA, providing that a violation of this IPIPA constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1, Schnucks' violation of the IPIPA and other pertinent statutes is also a violation of pertinent state consumer protection law.

JURY TRIAL DEMAND

86. Plaintiffs and class members demand a jury trial as to all claims and issues triable of right by a jury.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Members of the proposed Classes pray that this Honorable Court do the following:

A. Certify the matter as a class action pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure and order that notice be provided to all Class Members;

B. Designate Plaintiffs as representative of the Classes and the undersigned counsel as Class Counsel;

C. Award Plaintiffs and the Classes compensatory and punitive damages in an amount to be determined by the trier of fact;

D. Award Plaintiffs and the Classes statutory interest and penalties;

E. Award Plaintiffs and the Classes appropriate injunctive and/or declaratory relief;

F. Award Plaintiffs and the Classes their costs, prejudgment interest, and attorney fees; and

G. Grant such other relief as is just and proper.

Respectfully submitted,

By: /s/John J. Driscoll

John J. Driscoll, #54729MO
Christopher J. Quinn, #41883MO
Jeffrey Schultz, #6270576
The Driscoll Firm, P.C.
211 N. Broadway, 40th Floor
St. Louis, Missouri 63102
314-932-3232 telephone
314-932-3233 facsimile
Attorneys for Plaintiffs